Matthew Bishop, bishop@cs.ucdavis.edu
Deborah Frincke, deborah.frincke@pnl.com

CyberCIEGE: Gaming for Information Assurance

Cynthia E. Irvine and Michael F. Thompson
Naval Postgraduate School

Ken Allen
Rivermind

Cybersecurity students need to understand both the impact that poor security choices can have on an organization's health and the concrete steps that can improve security within it. In short, they must understand information assurance (IA) principles and how to apply them. Unfortunately, a disconnect often exists between principles and practice. Students sometimes feel that principles are boring or irrelevant, but without them, they can't go beyond "cookbook" remedies. In contrast, the competitive nature of matching wits with cyberadversaries can be stimulating, but with perceptions molded by hyperbolic news accounts, students can find critical conceptual issues elusive. As in many disciplines, effective information security requires both a practical and tacit understanding of the science and art of security engineering. Laboratory experiments can help convey these concepts, but a wide range of large-scale, realistic experiments would be too costly for most classrooms. Simulations thus provide a helpful alternative.

To address the need for realistic laboratory simulations, educators and researchers have begun exploring the use of games for purposes other than entertainment, such as for education. By capturing students' imaginations and generating a sense of competition, games provide a stimulating environment in which the participant has a stake in the outcome. This emotional investment makes the student an active learner, and the visualization associated with a game can often help to teach or reinforce concepts.

CyberCIEGE is a high-end, commercial-quality video game developed jointly by Rivermind and the Naval Postgraduate School's Center for Information Systems Security Studies and Research.[1–3] This dynamic, extensible game adheres to IA principles to help teach key concepts and practices.

Resource-management simulations

CyberCIEGE is a resource-management simulation in which the player assumes the role of a decision maker for an IT-dependent organization. The objective is to keep the organization's virtual users happy and productive while providing the necessary security measures to protect valuable information assets. Players face a limitless number of potential scenarios in which they have budgets and must make choices regarding procedural, technical, and physical security. With good choices, the organization prospers and the scenario advances; poor choices often result in disaster. Using the potential tension between strong security and user productivity, CyberCIEGE illustrates that many security choices involve risk management.

Games such as Electronic Arts' The Sims and Atari's RollerCoaster Tycoon illustrate the potential for resource-simulation tools to capture users' attention. They let players engage in planning and construction and observe the results of their choices. CyberCIEGE has a similar goal: players build and configure networks of computers, and their choices have visible effects on virtual users' ability to perform productive work and on attackers' ability to compromise assets. The scenarios strive to give students an emotional attachment to that which they build, thereby providing a more acute learning experience when poor decisions lead to loss.

Each CyberCIEGE scenario includes a briefing that describes an enterprise (for example, a business that manufactures bowling balls) and gives the player information about what's required to help make the enterprise successful. Within each scenario, the enterprise has a predefined security policy and set of users, assets, and user goals. The game's graphic design, shown in Figure 1, enhances each scenario's realism.

CyberCIEGE is designed to make it easy to create new scenarios that are tailored to specific audiences and topics. To even begin to cover the full range of cybersecurity topics requires numerous scenarios with different focus points and depths of detail. CyberCIEGE lets educators tailor scenarios for particular teaching objectives, and advanced students can even create their own scenarios. For example, a student might create an information security policy and imagine the kinds of tensions that could develop

Figure 1. CyberCIEGE virtual users at work. This scene depicts an enterprise for which the player must make IT choices that will affect virtual users.

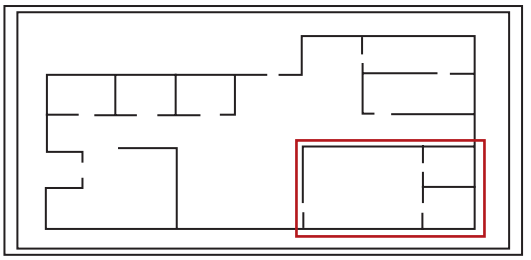

Figure 2. Office floor plan highlighting a zone. Players can provide zones with different physical levels of protection so that the enterprise security policy can be implemented through a combination of IT and physical mechanisms.

from trying to enforce it while letting users achieve their goals. This can help students learn that if they begin with an unenforceable security policy, no number of mechanisms will be sufficient for them to win the game.

CyberCIEGE elements

CyberCIEGE consists of several elements: a simulation engine, a scenario-definition language, a scenario-development tool, and a video-enhanced encyclopedia. The first three are used to construct CyberCIEGE scenarios, whereas the last can be used to augment the game's instructional capacity. Designers describe scenarios in a specialized scenario-definition language, which the underlying simulation engine interprets at game time. To simplify scenario development, CyberCEIGE also includes a scenario-definition tool.

Simulation engine

At its foundation, CyberCIEGE contains Rivermind's console-based Tybolt game engine, which is designed for both games and simulations. Tybolt is built around a multiplatform 3D graphics library that supports imported, standards-based objects and animations as well as Windows-like user interfaces within a fully 3D environment. The engine contains an artificial intelligence system, video-playback library, sound library, memory-management system, resource-management system, and real-time economic engine designed to support resource-management simulations.

Scenario-definition language

CyberCIEGE is built around a language through which scenario designers can express security-related risk management trade-offs, which the simulation engine interprets and presents as a simulation. Players' experiences and the consequences of their choices are functions of the scenario as expressed through the scenario-definition language. The language includes five major elements that allow security policies to be actualized in realistic networked environments.

Assets. Assets are various kinds of information that users must access to be productive—secret formulas, corporate accounting information, business plans, and marketing materials, for example. In a school, the assets might include student records, lesson plans, alumni lists, and admissions files. The enterprise pays a cost if an asset's secrecy or integrity is compromised; asset values present varying levels of motivation for attacks against them. Developers can associate *cost* and *motive* values with individual assets or entire sets (for example, "proprietary"), as well as tie values to other users with different access authorizations to those assets. Assets also have different secrecy, integrity, and availability values.

Users. Virtual users are typically employees whose productive work makes money for the enterprise. Their work goals sometimes include the need to access specific assets in various ways. Users also sometimes need to share assets, perhaps simultaneously accessing multiple assets. Users have different authorizations to access assets as defined by the enterprise's security policy. The student must provide the appropriate resources and environment to let users reach their goals. Goals can be abstract or specific and can directly affect the enterprise's balance sheet and employee morale.

Zones. Each scenario includes one or more physical zones that can control virtual users' physical move-

ments. When players purchase IT components, they place them within specific zones. Figure 2 illustrates a scenario in which the entire office is a zone; it can contain additional zones to which additional security measures are applied.

Conditions and triggers. The scenario designer defines conditions that the engine assesses during play, and specifies actions that occur as the result of combinations of conditions. For example, the player must perform a new set of actions when a virtual user receives a new asset goal. Designers use conditions and triggers to define winning and losing, as well as to specify what types of attacks occur (or don't occur) in response to various conditions. They can use pop-up windows and a moving message ticker at the bottom of the screen to show the player's progress, provide hints, or present complaints from unhappy users. Players then see different debriefing screens depending on how the game ends.

Objectives and phases. Scenarios can be divided into several phases, in which players must satisfy one or more objectives, defined in terms of conditions. Scenario designers can guide students' activities and provide incremental achievements by requiring them to achieve every objective in the current phase before transitioning to the next.

Scenario-development tool

Figure 3 shows a typical screen from the scenario-development tool. This form-based tool frees the designer from wrestling with the scenario-definition language's sophisticated and demanding syntax. It supports reusable libraries of scenario elements (for example, groups of users or assets),[4] and the development environment includes tools for compiling, validating, and running newly constructed scenarios as simulations.

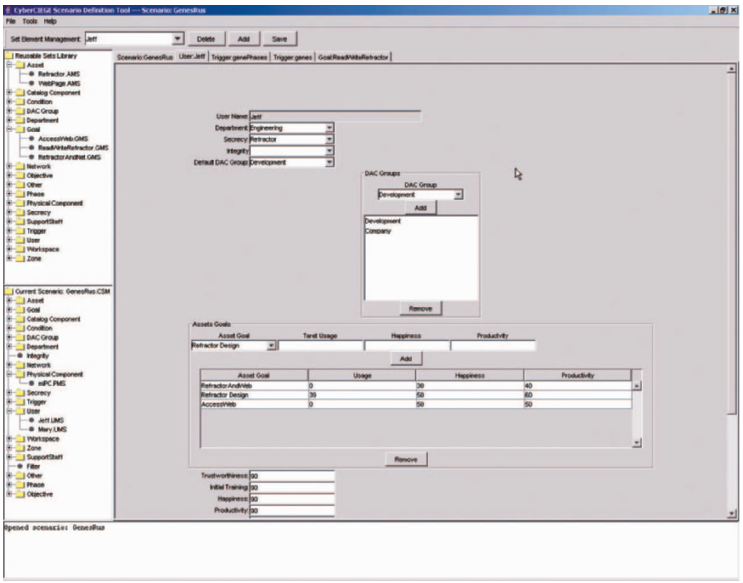

Figure 3. Scenario-development tool. The scenario-definition language's syntactic complexity can result in scenario definitions that are thousands of lines for even simple scenarios; the scenario-development tool hides this complexity and simplifies scenario construction.

Single scenarios can be well-defined IA teaching units. Combining them into campaigns lets teachers create coherent sequences of progressively more difficult scenarios or focused training units that cover multiple topics.[5]

Encyclopedia

Players can invoke the CyberCIEGE encyclopedia at any time. Context-sensitive encyclopedia entries explain how to play the game. Other entries describe a broad range of IA topics, including policies, passwords, network security devices, malicious software, and access control mechanisms. To complement the material in the encyclopedia, CyberCEIGE includes a set of movies that cover security policy, malicious software, firewalls, assurance, and how to use the game. The movies are designed to be understandable and entertaining to all audiences.

CyberCIEGE use

Every scenario starts with a briefing that describes the enterprise for which computer resources must be managed. Players are responsible for activities such as configuring and networking existing computer components, making physical and procedural security choices, hiring IT support staff, and purchasing specific components and connecting them to the networks.

With a limited budget, the player must make money for the enterprise by efficiently and securely managing the networks. This requires an understanding of all user goals—that is, each virtual user's needs for access to different assets. The users must have suitable computer components, software, network interconnections, and technical-support personnel to achieve their goals.

The player must create and maintain an environment in which assets are protected in accordance with the enterprise security policy. Failure to adequately protect the assets results in monetary losses to the enterprise due to both direct loss and lost user productivity. This involves several kinds of choices:

- component selection and deployment,
- component configuration,
- component interconnection using networks,
- user instruction and training,
- physical security restrictions, and
- user background-check levels.

These security choices affect the protections provided to the enterprise assets, which are subject to attack from vandals, disgruntled employees, professional attackers, incompetent users, and acts of nature.

Players typically construct networks and make policy-enforcement decisions prior to starting a simulation. Once the simulation begins, virtual users start creating and accessing their assets—sometimes in ways that make the assets vulnerable to attack.

During the game, which can be paused at any time, players can select and observe the status of a user's productivity and happiness. Users who are unable to achieve their goals become visibly agitated. This is intended to increase the player's sense of urgency—numerous unhappy users can create a stressful situation for the IT department.

The Naval Postgraduate School released a limited-distribution version of CyberCIEGE in February 2005, specifically for US government use. Rivermind then released the first commercial version in April. The CyberCIEGE Web site (http://cisr.nps.navy.mil/cyberciege.html) serves as a repository for scenarios created by NPS and other educators, as well as a place for end users to provide feedback. We hope to work with organizations to tailor CyberCIEGE to meet their specific teaching requirements, including developing new scenarios, extending the simulation, or adding new artwork.

The scenario-definition language contains triggers that result in output to an activity log, which teachers can use for assessing students and to identify topics for further instruction. We're working on a preliminary set of assessment tools for the logs to increase the system's value to educators. We're also beginning an effort to examine the human factors that might improve teaching success for the game among various student populations, which might differ according to age, gender, education, and other factors.

Advanced versions of CyberCIEGE could take several forms, including wireless and multiplayer versions. The current version contains no mobile users or wireless components. Adding such technologies to the existing simulation would significantly advance its ability to depict emerging architectures. The competitive and dynamic nature of a multiplayer version would further engage and challenge students as they worked to protect and provide services to their virtual organizations while finding and exploiting vulnerabilities in their competitors' systems. We're currently conducting preliminary research for a multiplayer version of CyberCIEGE. □

Acknowledgments

CyberCIEGE was sponsored by the US Navy, the Naval Education and Training Command, the Office of Naval Research, and the Office of the Secretary of Defense. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the sponsors' views. CyberCIEGE is a trademark of Rivermind.

References

1. C.E. Irvine and M. Thompson, "Teaching Objectives of a Simulation Game for Computer Security," *Proc. Informing Science and Information Technology Joint Conf.*, Informing Science Institute, June 2003, pp. 779–791.
2. C.E. Irvine and M. Thompson, "Expressing an Information Security Policy within a Security Simulation Game," *Proc. 6th Workshop Education in Computer Security* (WECS6), Naval Postgraduate School, 2004, pp. 43–49; http://cisr.nps.navy.mil/downloads/WECS6_Proceedings.pdf.
3. C.E. Irvine, M.F. Thompson, and K. Allen, "CyberCIEGE: An Information Assurance Teaching Tool for Training and Awareness," *Proc. Federal Information Systems Security Educators' Association Conf.* (FISSEA 2005), US Nat'l Inst. Standards and Technology, 2005; http://csrc.nist.gov/organizations/fissea/conference/2005/agenda-and-presentations.html.
4. K.W. Johns, *Toward Managing and Automating CyberCIEGE Scenario Definition File Creation*, masters thesis, Naval Postgraduate School, Monterey, Calif., June 2004.
5. T.L. Teo, *Scenario Selection and Student Selection Modules for CyberCIEGE*, masters thesis, Naval Postgraduate School, Monterey, Calif., Dec. 2003.

Cynthia E. Irvine *is a professor in the Department of Computer Science at the Naval Postgraduate School. Her research interests include high-assurance systems, security architectures, and information assurance education. Irvine received a PhD in astronomy from Case Western Reserve University. She is a senior member of the IEEE and director of the Center for Information Systems Security Studies and Research at NPS. Contact her at irvine@nps.edu.*

Michael F. Thompson *is a research assistant at the Naval Postgraduate School. His research interests include high assurance computer and network security. Thompson received a BS in electrical engineering from Marquette University. He is also the director of systems security engineering for Aesec Corporation. Contact him at mfthomps@nps.edu.*

Ken Allen *is cofounder and chief financial officer of Rivermind. His research interests include advanced simulations, artificial intelligence. and real-time 3D renedering. Allen received an MS in computer science from California State University, Long Beach. He has created and shipped several top-selling video games. Contact him at kallen@rivermind.com.*